

Progressions in Every Two-Coloration of Z_n

H. Y. SONG, H. TAYLOR, AND S. W. GOLOMB

*Communication Sciences Institute, Department of EE-Systems,
University of Southern California, Los Angeles, California 90089-0272*

Received June 15, 1990

For each positive integer n , $G(n)$ is defined to be the largest integer k such that no matter how Z_n is two-colored, some progression $a, a + d, a + 2d, \dots, a + (k - 1)d$ of k distinct elements of Z_n will appear in one color. Our main theorem shows constructively that if Z_n can be two-colored in such a way that the longest monochrome progression has m distinct terms mod n and any monochrome progression of k distinct terms with common difference $d \not\equiv 0 \pmod{n}$ has the property that $kd \not\equiv 0 \pmod{n}$, then $G(rn) \leq m$ for $1 \leq r \leq m$ and $G(rn) \leq r$ for $r > m$. One lower bound on $G(n)$ says $G(rn) \geq G(n)$ for $r \geq 1$ and $n \geq 1$. Two main results with corollaries, a “quadratic-residue coloration” on Z_p for p a prime, and the *van der Waerden* numbers $W(k)$ for $2 \leq k \leq 5$, together with a computer search, have been used to determine the exact value of $G(n)$ for $1 \leq n \leq 53$, for all primes up to 71, and for a few more cases, the highest of which is $G(695) = 5$ which guarantees that $W(6) \geq 696$. © 1992 Academic Press, Inc.

1. INTRODUCTION

The main purpose of this paper is to determine the exact value of $G(n)$ for each positive integer n , which has been proposed initially by Professor S. W. Golomb.

DEFINITION 1.1. For each positive integer n , let Z_n be the set of integers modulo n . Then, $G(n)$ is the largest integer k such that no matter how Z_n is two-colored, some progression $a, a + d, a + 2d, \dots, a + (k - 1)d$ of k distinct elements of Z_n (we call this a k -term circular progression) will appear in one color.

Our main theorem concerning the upper bound on $G(n)$ is proved in the next section. So is one lemma on the lower bound on $G(n)$. It turns out that the value of $G(p)$ for p a prime is crucial to determining G for many other values.

R. Graham, B. Rothschild, and J. Spencer [1] reported all the known values of $W(k)$, known as *van der Waerden numbers*, which are $W(2) = 3$, $W(3) = 9$, $W(4) = 35$, and $W(5) = 178$. $W(k)$ is defined to be the minimal

TABLE I
All the Known Values of $G(n)$

n	$G(n)$	Upper Bound	Lower Bound
1	1		
2 = prime	1		
3 = prime	2	QR coloration	$n \geq W(2)$
4 = 2 · 2	2	Cor.2.3	$n \geq W(2)$
5 = prime	3	QR coloration	Cor.2.2
6 = 2 · 3	2		Cor.2.5
7 = prime	3	QR coloration	Cor.2.2
8 = 2 · 2 · 2	2	Cor.2.3	$n \geq W(2)$
9 = 3 ²	3	Cor.2.1	$n \geq W(3)$
10 = 2 · 5	3		Cor.2.5
11 = prime	3	QR coloration	Cor.2.2
12 = 2 · 2 · 3	3	Cor.2.3	$n \geq W(3)$
13 = prime	4	QR coloration	Cor.2.2
14 = 2 · 7	3		Cor.2.5
15 = 3 · 5	3		Cor.2.5
16 = 2 · 2 · 4	4	Cor.2.3	s.t.=0.5 sec.
17 = prime	5	QR coloration	s.t.=0.3 sec.
18 = 2 · 3 · 3	3	Cor.2.3	$n \geq W(3)$
19 = prime	4	QR coloration	Cor.2.2
20 = 4 · 5	4	Cor.2.1	1 min. ≤ s.t. ≤ 2 min.
21 = 3 · 7	3		Cor.2.5
22 = 2 · 11	3		Cor.2.5
23 = prime	5	QR coloration	s.t.= 1 sec.
24 = 2 · 4 · 3	4	Cor.2.3	1 min. ≤ s.t. ≤ 2 min.
25 = 5 ²	5	Cor.2.1	1 min. ≤ s.t. ≤ 2 min.
26 = 2 · 13	4		Cor.2.5
27 = 3 · 9	4	Cor.2.4	1 min. ≤ s.t. ≤ 2 min.
28 = 4 · 7	4	Cor.2.1	1 min. ≤ s.t. ≤ 2 min.
29 = prime	4	QR coloration	Cor.2.2
30 = 2 · 15	4	Cor.2.4	1 min. ≤ s.t. ≤ 2 min.
31 = prime	4	QR coloration	Cor.2.2
32 = 2 · 4 · 4	4	Cor.2.3	$G(2 \cdot 16) \geq G(16)$
33 = 3 · 11	3		Cor.2.5
34 = 2 · 17	5		Cor.2.5
35 = 5 · 7	5	Cor.2.1	1 min. ≤ s.t. ≤ 2 min.
36 = 3 · 12	4	Cor.2.4	$n \geq W(4)$
37 = prime	4	QR coloration	$n \geq W(4)$
38 = 2 · 19	4		Cor.2.5
39 = 3 · 13	4		Cor.2.5
40 = 2 · 20	4	Cor.2.4	$G(2 \cdot 20) \geq G(20)$
41 = prime	5	QR coloration	s.t. ≤ 1 min.

Note. $n=54$ is the smallest unsettled case. $n=695$ is the biggest integer for which $G(n)$ is known.

TABLE I—Continued

n	$G(n)$	Upper Bound	Lower Bound
$42 = 3 \cdot 14$	4	Cor.2.4	$n \geq W(4)$
$43 = \text{prime}$	5	QR coloration	s.t.=1 min.
$44 = 4 \cdot 11$	4	Cor.2.1	$n \geq W(4)$
$45 = 3 \cdot 15$	4	Cor.2.4	$n \geq W(4)$
$46 = 2 \cdot 23$	5		Cor.2.5
$47 = \text{prime}$	5	QR coloration	Cor.2.2
$48 = 4 \cdot 12$	4	Cor.2.4	$G(2 \cdot 24) \geq G(24)$
$49 = 7 \cdot 7$	6	$G \leq 6, \text{ s.t.} \leq 1 \text{ min.}$	$G \geq 6, \text{ 10 hrs.} \leq \text{s.t.} \leq 12 \text{ hrs.}$
$50 = 2 \cdot 5 \cdot 5$	5	Cor.2.3	$G(2 \cdot 25) \geq G(25)$
$51 = 3 \cdot 17$	5		Cor.2.5
$52 = 4 \cdot 13$	4		Cor.2.5
$53 = \text{prime}$	6	QR coloration	s.t.=5 hrs.
$54 = 6 \cdot 9$?	$G(6 \cdot 9) \leq 6$	$G(2 \cdot 27) \geq G(27) = 4$
$55 = 5 \cdot 11$?	$G(5 \cdot 11) \leq 5$	$G(55) \geq 4, \text{ by } n \geq W(4)$
$56 = 4 \cdot 14$	4	Cor.2.4	$n \geq W(4)$
$57 = 3 \cdot 19$	4		Cor.2.5
$58 = 2 \cdot 29$	4		Cor.2.5
$59 = \text{prime}$	5	QR coloration	Cor.2.2
$60 = 4 \cdot 15$	4	Cor.2.4	$G(3 \cdot 20) \geq G(20)$
$61 = \text{prime}$	6	QR coloration	2 days \leq s.t. \leq 3 days
$62 = 2 \cdot 31$	4		Cor.2.5
$66 = 3 \cdot 22$	4	Cor.2.4	$n \geq W(4)$
$67 = \text{prime}$	6	QR coloration	7 days \leq s.t. \leq 10 days
$68 = 4 \cdot 17$	5		Cor.2.5
$69 = 3 \cdot 23$	5		Cor.2.5
$71 = \text{prime}$	6	s.t. $\leq 5 \text{ min.}$	7 days \leq s.t. \leq 10 days
$73 = \text{prime}$?	$G \leq 6, \text{ s.t.} \leq 5 \text{ min.}$	$G \geq 5, \text{ by Cor.2.2}$
$74 = 2 \cdot 37$	4		Cor.2.5
$76 = 4 \cdot 19$	4		Cor.2.5
$80 = 4 \cdot 20$	4	Cor.2.4	$n \geq W(4)$
$85 = 5 \cdot 17$	5		Cor.2.5
$86 = 2 \cdot 43$	5		Cor.2.5
$87 = 3 \cdot 29$	4		Cor.2.5
$88 = 4 \cdot 22$	4	Cor.2.4	$n \geq W(4)$
$92 = 4 \cdot 23$	5		Cor.2.5
$93 = 3 \cdot 31$	4		Cor.2.5
$94 = 2 \cdot 47$	5		Cor.2.5
$111 = 3 \cdot 37$	4		Cor.2.5
$113 = \text{prime}$	5	QR coloration	Cor.2.2
$115 = 5 \cdot 23$	5		Cor.2.5

Table continued

TABLE I—Continued

n	$G(n)$	Upper Bound	Lower Bound
$116 = 4 \cdot 29$	4		Cor.2.5
$118 = 2 \cdot 59$	5		Cor.2.5
$122 = 2 \cdot 61$	6		Cor.2.5
$124 = 4 \cdot 31$	4		Cor.2.5
$129 = 3 \cdot 43$	5		Cor.2.5
$134 = 2 \cdot 67$	6		Cor.2.5
$139 = \text{prime}$	5	QR coloration	Cor.2.2
$141 = 3 \cdot 47$	5		Cor.2.5
$142 = 2 \cdot 71$	6		Cor.2.5
$148 = 4 \cdot 37$	4		Cor.2.5
$172 = 4 \cdot 43$	5		Cor.2.5
$177 = 3 \cdot 59$	5		Cor.2.5
$183 = 3 \cdot 61$	6		Cor.2.5
$185 = 5 \cdot 37$	5	Cor.2.1	$n \geq W(5)$
$188 = 4 \cdot 47$	5		Cor.2.5
$201 = 3 \cdot 67$	6		Cor.2.5
$205 = 5 \cdot 41$	5	Cor.2.1	$n \geq W(5)$
$213 = 3 \cdot 71$	6		Cor.2.5
$215 = 5 \cdot 43$	5		Cor.2.5
$226 = 2 \cdot 113$	5		Cor.2.5
$235 = 5 \cdot 47$	5		Cor.2.5
$236 = 4 \cdot 59$	5		Cor.2.5
$244 = 4 \cdot 61$	6		Cor.2.5
$268 = 4 \cdot 67$	6		Cor.2.5
$278 = 2 \cdot 139$	5		Cor.2.5
$284 = 4 \cdot 71$	6		Cor.2.5
$295 = 5 \cdot 59$	5		Cor.2.5
$305 = 5 \cdot 61$	6		Cor.2.5
$335 = 5 \cdot 67$	6		Cor.2.5
$339 = 3 \cdot 113$	5		Cor.2.5
$355 = 5 \cdot 71$	6		Cor.2.5
$366 = 6 \cdot 61$	6		Cor.2.5
$373 = \text{prime}$?	$G \leq 6$, by QR coloration	$G \geq 5$, since $n \geq W(5)$
$402 = 6 \cdot 67$	6		Cor.2.5
$417 = 3 \cdot 139$	5		Cor.2.5
$426 = 6 \cdot 71$	6		Cor.2.5
$452 = 4 \cdot 113$	5		Cor.2.5
$565 = 5 \cdot 113$	5		Cor.2.5
$556 = 4 \cdot 139$	5		Cor.2.5
$695 = 5 \cdot 139$	5		Cor.2.5

integer n such that no matter how the set of integers $\{1, 2, \dots, n\}$ is two-colored, it contains a k -term arithmetic progression in one color. Since the existence of a k -term arithmetic progression in a set of consecutive integers implies the existence of a k -term circular progression in Z_n , we have one easy lower bound on G given as $G(n) \geq k$ for any $n \geq W(k)$.

While $W(k)$ is a strictly increasing function on k , the function $G(n)$ has ups and downs such as, for example, $G(16)=4$, $G(17)=5$, and $G(18)=3$ (Table I). It seems to be fluctuating more irregularly as n grows. However, the fluctuation of $G(n)$ is lower-bounded by $W(k)$ and also by the lower bound in Lemma 2.1.

For p a small prime, it seems that the coloration of each integer in Z_p according to whether it is a quadratic residue or not, with any color on the integer 0 (we call this a QR coloration) gives a rather tight upper bound on $G(p)$. It is the result of a computer search that $n=71$ and 73 are the first two primes for which the value of G is less than the upper bound given by the QR coloration.

The computer search, together with all of the above-mentioned methods, has been used to determine $G(n)$ for all the primes less than 73, all composite numbers less than 54, and a few more sporadic cases, the highest of which is $G(695)=5$, from which it follows that $W(6)$ is at least 696.

2. BOUNDS ON G

THEOREM 2.1. *Suppose there exists a two-coloration on Z_n in which the longest monochrome progression has m distinct terms mod n and any monochrome progression $a, a+d, a+2d, \dots, a+(k-1)d$ of k terms all distinct modulo n having difference $d \not\equiv 0 \pmod{n}$ has the property that $kd \not\equiv 0 \pmod{n}$. Then, we have $G(rn) \leq m$ for $1 \leq r \leq m$, and $G(rn) \leq r$ for $r > m$.*

Proof. To prove Theorem 2.1 we construct a two-coloration on Z_{rn} by repeating the given two-coloration on Z_n periodically r times. That is, for each $y \in Z_{rn}$, we find the unique $x \in Z_n$ such that $y \equiv x \pmod{n}$ and give y the same color as x .

First, if a monochrome progression in Z_{rn} has common difference $d \equiv 0 \pmod{n}$, then it has exactly r terms, all distinct modulo rn , which form a regular r -gon. For $r > m$, it is the only case where we can find a monochrome progression in Z_{rn} having more than m terms, since we prove the claim that any other monochrome progressions in Z_{rn} having common difference $d \not\equiv 0 \pmod{n}$ have at most m distinct terms mod rn , whether $r > m$ or $1 \leq r \leq m$.

To show the above claim, assume that there exists a monochrome

$(m+1)$ -term circular progression in the extended two-coloration on Z_{rn} having difference $d \not\equiv 0 \pmod{n}$, i.e.,

$$a, a+d, a+2d, \dots, a+(m-1)d, a+md.$$

By mapping each term in the above progression down to Z_n , we have a progression in Z_n ,

$$a_0, a_1, a_2, \dots, a_{m-1}, a_m,$$

where $a_i \equiv a + id \pmod{n}$ for $0 \leq i \leq m$. All of the a_i 's above have the same color and, since they form a progression of more than m terms, they cannot all be distinct mod n . Therefore we can choose i and j such that $0 \leq i < j \leq m$ and $a_i, a_{i+1}, \dots, a_{j-1}$ are all distinct mod n but $a_i \equiv a_j \pmod{n}$. This implies that

$$a + id \equiv a + jd \pmod{n},$$

or

$$(j-i)d \equiv 0 \pmod{n}.$$

If $j-i=1$, we have $d \equiv 0 \pmod{n}$, contrary to our assumption in the claim. If $j-i=k > 1$, we have a monochrome progression of k terms all distinct mod n , violating the property that $kd \not\equiv 0 \pmod{n}$. Thus we have proved that $G(rn) \leq m$ for $1 \leq r \leq m$, and $G(rn) \leq r$ for $r > m$. ■

COROLLARY 2.1. *Let p be a prime and $m < p$. If Z_p can be two-colored in such a way that the longest monochrome progression has m distinct terms mod p , then $G(rp) \leq m$ for $1 \leq r \leq m$, and $G(rp) \leq r$ for $r > m$.*

COROLLARY 2.2. *For a prime p , we have:*

- $G(p) \geq 3$, if $p \geq 5$ is a prime.
- $G(p) \geq 4$, if $p \geq 13$ is a prime.
- $G(p) \geq 5$, if $p \geq 47$ is a prime.

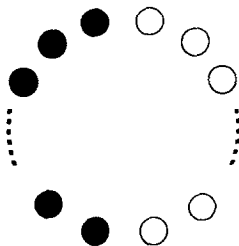
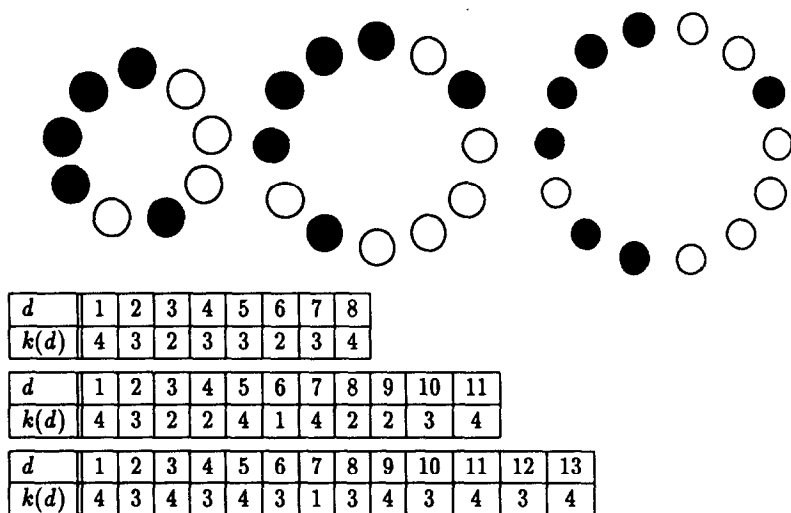


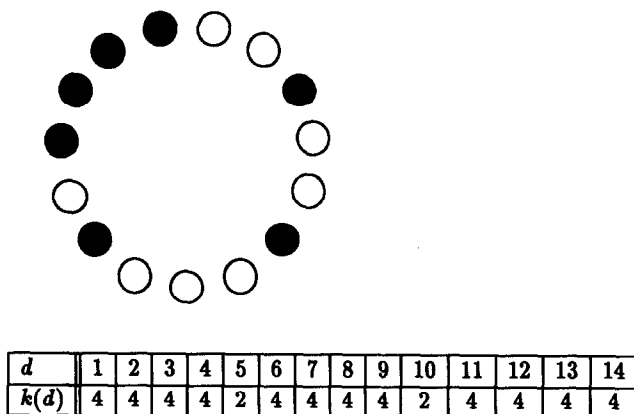
FIG. 1. The two-coloration on Z_{2m} proposed in Corollary 2.3.

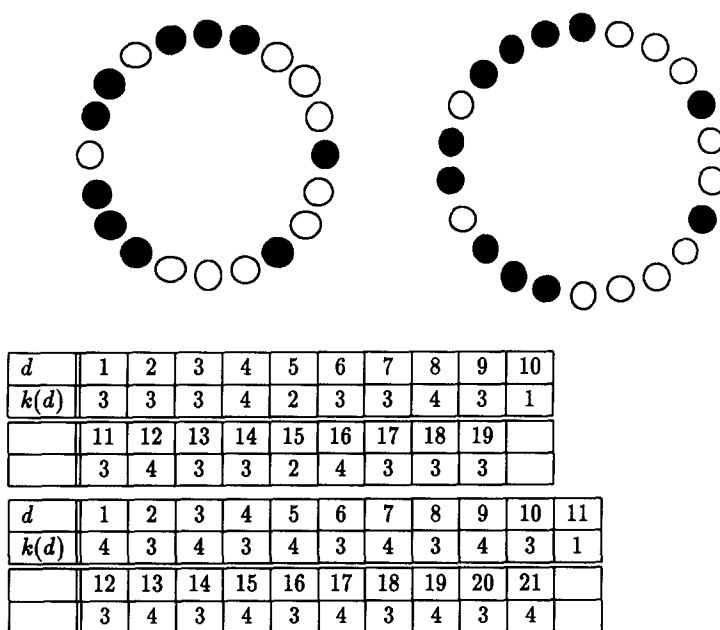
FIG. 2. Two-colorations on Z_9 , Z_{12} , and Z_{14} with corresponding tables for $k(d)$.

Proof. Recall that $W(3)=9$, $W(4)=35$, and $W(5)=178$. If $G(p)=2$ for $p \geq 5$, then, by Corollary 2.1, we have $G(2p) \leq 2$, where $2p \geq 10$. This contradicts $G(n) \geq 3$ for $n \geq 9$ by $W(3)=9$. Similarly, we have the other two lower bounds. ■

COROLLARY 2.3. Let n be even and write $n=2m$, where $m \geq 1$. Then, $G(2mr) \leq m$ for $1 \leq r \leq m$, and $G(2mr) \leq r$ for $r > m$.

Proof. Let Z_{2m} be two-colored in such a way that $0, 1, 2, \dots, m-1$ have one color and $m, m+1, \dots, 2m-1$ have the other as shown in Fig. 1. It is

FIG. 3. A two-coloration on Z_{15} with $k(d)$ value for each d .

FIG. 4. Two-colorations on Z_{20} and Z_{22} with corresponding tables for $k(d)$.

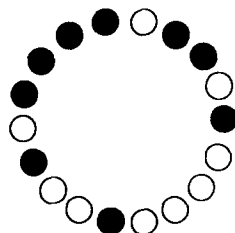
obvious that m is the maximum number of any monochrome progression. If there exists a monochrome progression of k distinct terms with $d \not\equiv 0 \pmod{2m}$ having the property that $kd \equiv 0 \pmod{2m}$ in a two-coloration on Z_{2m} , then we can find a regular k -gon having k monochrome vertices, which is easily seen to be impossible in the coloration of Fig. 1. Therefore, all the conditions of the theorem are satisfied. ■

DEFINITION 2.2. For any integer d and a given coloration on Z_n , define $k(d)$ to be the largest integer k such that we can find a monochromatic k -term circular progression in the coloration, having common difference d .

Figures 2, 3, 4, and 5 show values of $k(d)$ for the given two-coloration

d	1	2	3	4	5	6	7	8	9
$k(d)$	4	3	3	3	6	2	3	4	1

d	10	11	12	13	14	15	16	17	
$k(d)$	4	3	2	6	3	3	3	4	

FIG. 5. A two-coloration on Z_{18} in which there exist some six-term monochrome circular progressions having common difference 5.

on Z_n and each d from 1 to $n-1$. Note that, for $n=9, 12, 14, 15, 20$, and 22 , the two-coloration shown in the figure satisfies the condition $kd \not\equiv 0 \pmod{n}$ for any $1 \leq d \leq n-1$ and has at most $m=4$ terms all distinct mod n in any monochromatic progression. The two-coloration on Z_{18} in Fig. 5 satisfies the condition that $kd \not\equiv 0 \pmod{18}$ for any k -term monochrome circular progression with at most $m=6$ distinct terms in any monochrome progression.

COROLLARY 2.4. For $1 \leq r \leq 4$, we have $G(9r) \leq 4$, $G(12r) \leq 4$, $G(14r) \leq 4$, $G(15r) \leq 4$, $G(20r) \leq 4$, and $G(22r) \leq 4$.

LEMMA 2.1. For $r \geq 1$ and $n \geq 1$, we have $G(rn) \geq G(n)$.

Proof. Suppose the longest monochrome progression in a two-coloration on Z_{rn} has k distinct terms modulo rn . Now, we can obtain a two-coloration on Z_n by taking every r th term, in which the number of terms of the longest monochrome progression is less than or equal to the number of k distinct terms modulo n . ■

COROLLARY 2.5. If $1 \leq r \leq G(p)$ for p a prime, then $G(rp) = G(p)$.

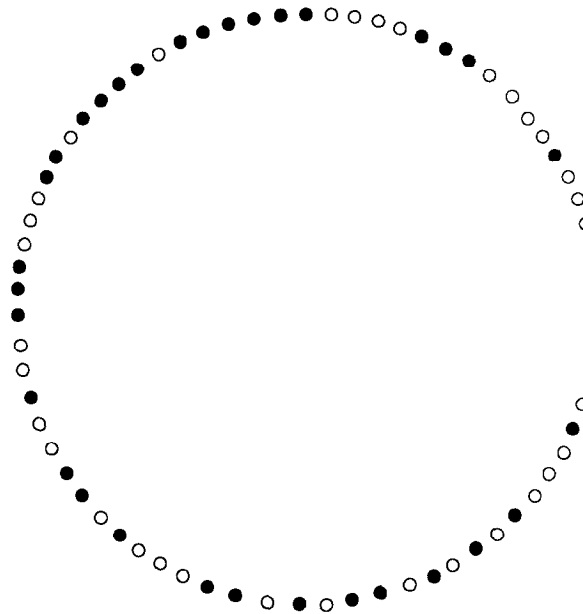
Proof. By Corollary 2.1, $G(rp) \leq G(p)$. On the other hand, by the above lemma, $G(rp) \geq G(p)$. ■

3. CONCLUSION

A computer search has been done to determine the exact value of $G(p)$ for primes p up to 71. Note that $G(71) \geq 5$ by Corollary 2.2. It took approximately 10 days of CPU time (Sun-3/60) to conclude that every possible five-term circular progression in one color forces a six-term circular progression in one color in Z_{71} . On the other hand, the search to show that $G(71) \leq 6$ took less than 5 min of CPU time, since the search stopped as soon as it found a coloring on all 71 integers without a monochrome seven-term circular progression (Fig. 6).

For some n for which $G(n) \leq 4$, another exhaustive computer search has been done to find examples of two-colorations which satisfy the conditions of Theorem 2.1 with $m=4$. For each $n=9, 12, 14, 15, 20$, and 22 , the two-coloration shown in Figs. 2, 3, and 4 turned out to be the essentially unique example satisfying the conditions of the theorem with $m=4$. For $n=16, 18, 21, 24, 26$, and 27 , all of the two-colorations in which the longest monochrome progression has $m=4$ distinct terms fail to satisfy the conditions of the theorem.¹ Each case took less than 2 min of CPU time.

¹ The same is true for $n=18$ and 27 with $m=5$.



d	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$k(d)$	6	6	5	6	5	6	6	6	5	6	5	6	6	5
d	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$k(d)$	6	6	6	6	6	6	5	6	5	5	5	6	6	5
d	29	30	31	32	33	34	35	36	37	38	39	40	41	42
$k(d)$	6	5	6	6	6	5	5	5	5	6	6	6	5	6
d	43	44	45	46	47	48	49	50	51	52	53	54	55	56
$k(d)$	5	6	6	5	5	5	6	5	6	6	6	6	6	6
d	57	58	59	60	61	62	63	64	65	66	67	68	69	70
$k(d)$	5	6	6	5	6	5	6	6	6	5	6	5	6	6

FIG. 6. A two-coloration on Z_{71} without any monochrome seven-term circular progression, found by computer.

From our main theorem, lemma, corollaries, the known values of $W(k)$, and the QR coloration, $G(n)$ for various values of n can be determined without exhaustive computer search, and these are listed in Table I. When the bound is determined by computer search, the actual CPU search time (s.t.) for each case is listed.

From the QR colorations on Z_p for $p=71$ and 73 , mentioned in the Introduction, we have $G(71)\leq 7$ and $G(73)\leq 9$. Note that $71\equiv -1$

(mod 4), $73 \equiv 1 \pmod{4}$, and the runs of quadratic residues look quite different in the two cases. It turned out from the search that $p = 71$ and 73 are the first two primes for which $G(p)$ is less than the value given by the QR coloration.

One rough guess for $W(6)$ from the known values of $W(k)$, $2 \leq k \leq 5$, is $W(6) \stackrel{?}{\cong} 6W(5) = 1068$. All we are sure of is that

$$W(6) \geq 695 + 1,$$

since $G(695) = G(5 \cdot 139) = 5$. The values of prime p for which $G(p)$ is known to be either 5 or 6 are 373, 349, 257, 229, 199, 181, 179, 173, For those primes, $G(p) \geq 5$ by Corollary 2.2 and $G(p) \leq 6$ by the QR coloration. Since $G(373) \leq 6$, from Theorem 2.1, we have $G(6 \cdot 373) = G(2238) \leq 6$ and, hence, we are sure also that

$$W(7) \geq 2238 + 1.$$

For the large values of n , the tightest upper bound on $G(n)$ comes from the lower bound on $W(k)$ which is proved constructively in [1]:

$$\text{For each prime } p, \quad W(p+1) \geq p2^p.$$

By arranging the two-coloration on the set of integers $1, 2, \dots, p2^p$ in a circle and considering the possibility that the length of a monochrome p -term arithmetic progression can now be at most doubled, we have, for each prime p :

$$\text{For all } n \leq p2^p, \quad G(n) \leq 2p.$$

REFERENCES

1. R. L. GRAHAM, B. L. ROTHCHILD, AND J. H. SPENCER, "Ramsey Theory," 2nd ed., Wiley, New York, 1990.
2. D. M. BURTON, "Elementary Number Theory," Allyn & Bacon, Boston, 1980.
3. N. WIRTH, "Algorithms + Data Structure = Programs," Prentice-Hall, Englewood Cliffs, NJ, 1976.